UNITED STATES DISTRICT COURT
EASTERN DISTRICT OF WISCONSIN

UNITED STATES OF AMERICA,

Plaintiff,

v. Case No. 13-CR-120

PAUL D. CASE,

Defendant.

REPLY BRIEF IN SUPPORT OF THE DEFENNDANT'S OBJECTIONS

1.0 Introduction

The government in its response asserts that all of its pre-affidavit activities were lawful, and presumably for this reason does not address either the independent source issue or the inevitable discovery issue. But the government does explicitly assert that its online covert employee is a real person whose covert activities make it necessary that he not be identified in a public affidavit.[1] This

[1] In prior pleadings Case assumed, based on the complete absence of any description of the Online Covert Employee (OCE-5023) and the methodology that he used, that he was fictitious and that OCE represented a computer operating a questionable search program. This was partially supported in an opinion filed on January 10, 2014, in which the Hon. Terrence W. Boyle (E.D.N.C.) noted that the Online Covert Employee was a non-human source, when he distinguished a "FBI confidential human source from an "FBI online covert employee." *United States v. Sheikh*, 2014 U.S. Dist. LEXIS 3090 at 2. Unfortunately, Case's assumption and the coy reticence of the government led to exhaustive research on the reliability of the RoundUp computer program, hundreds of pages of pleadings and exhibits and the employment of computer experts. All of this could have been avoided had the government earlier disclosed that its Online Covert Employee was an actual person whose other covert activity required anonymity.

Counsel for Case does not respond to the government's stridently expressed opinions in the hope that the dialectic in future submissions will return to the civility for which this District is known.

assertion requires that Case explore its consequences and compels that Case agree with the Court that Case's original focus on *Franks v. Delaware* analysis obscures the real issue.[2]

[2] In a sense the omissions and concealment in the affidavit raise a quasi-*Franks* issue which can only be resolved at an evidentiary hearing. At the hearing Case would establish (1) that Roundup was the program operated by the FBI computer which identified and downloaded the Case files on November 24-25, 2012; (2) the computer was untended by OCE-5023, or by any other person, during the time between 2:11 AM on November 24, 2012 and 3:33 AM on November 25, 2012; (3) whether the FBI used RoundUp, or any other computer program, to access the Case computer at any time prior to 2:11 AM on November 24, 2012 or any time between 3:33 AM on November 25, 2012 and the date on which the affidavit for the search and seizure of Case's computer was signed. A former associate at Shellow, Shellow & Glynn wrote,

> A Trojan horse program "is a malicious code concealed within an apparently harmless [computer] program that hides its true function." U.S. DEP'T OF JUSTICE, NAT'L INST, OF JUSTICE, INVESTIGATIONS INVOLVING THE INTERNET AND COMPUTER NETWORKS 55 (2007), *available at* http://www.ncjrs.gov/pdffiles1/nij/210798.pdf. Trojan Horse programs are routinely used by cybercriminals to steal information from unwary computer users or to take control of their computers. *See id.* at 1. As Timothy C. MacDonnell notes, they could also be used by law enforcement:
>
> > In the context of the home, the government could send an email to a suspect that contains a 'Trojan horse" program. Once the email was opened the program could be downloaded to the suspect's computer without his knowledge. The program would search the target computer for the hash value of known contraband files. If the program encountered a contraband file, it would alert law enforcement.
>
> Timothy C. MacDonnell, *Orwellian Ramifications: The Contraband Exception to the Fourth Amendment*, 41 U. MEM. L. REV. 299, 346-47 (2010) (footnotes omitted); *see id.* at 347 n.335 (noting that Trojan Horse programs let the operator of the software retrieve user names and passwords stored on the target computer and "find, view, copy and delete files," among other things).

Susan W. Brenner, Distinguished Professor of Law and Technology, University of Dayton School of Law, *Fourth Amendment Future: Remote Computer Searches and the Use of Virtual Force*, 81 Miss. L. J. 1229, 1231n. 14 (Symposium 2012).

Rather, Case's basic thesis is simple and straightforward: The workproduct of an unidentified computer program running on an untended computer cannot be the basis for a finding of probable cause.[3]

The foundation for the finding of probable cause by the Magistrate Judge lies on the following assertions in the affidavit that on November 24 and 25, 2012 the OCE downloaded five files of child pornography from Paul Case's computer.

> 25. On November 24, 2012, around 2:11 a.m. Central Standard Time ("CST"), Online Covert Employee 5023 ("OCE-5023"), acting in an undercover capacity, conducted investigations into the sharing of child pornography files on the Ares P2P file sharing network. During this time, OCE-5023 identified a computer with the IP address 174.102.233.53 with at least seven files of investigative interest available for download.
>
> 27. Between 02:11 a.m. CST on November 24, 2012, and 03:33 a.m. CST on November 25, 2012, OCE-5023 successfully completed downloads of five files containing child pornography from the computer at IP address 174.102.233.53, including the following three files:

The files that followed all described child pornography. R. 1:15-17. *N.B.* Page 5 of the search warrant affidavit was not filed.

2.0 FACTS

1. The RoundUp computer program was used on November 24, 2012 and November 25, 2012 to search Case's computer files and identify and download child pornography.[4]

---

[3] This issue is discussed more fully and articulately in an article from The Institute for Security, Technology, and Society at Dartmouth College and the Franklin Pierce Law Center by Sergey Bratus, Ashlyn Lembree and Anna Shubina, *Software on the Witness Stand: What Should it Take for Us to Trust It?* http://www.cs.dartmouth.edu/~sergey/trusting-e-evidence.pdf. Case has copied this article and submitted it as Exhibit 1 to this reply. It differs from the online version in that it is paginated.

[4] AUSA Benjamin Proctor has admitted that "[m]y understanding is that RoundUp was used as part of this investigation" Document 32-2.

2. This computer identification and downloading of Case's files was untended by OCE-5023.[5]

3. The FBI affiant in the affidavit in support of warrant to seize and search Case's computer did not identify the computer program which identified and downloaded the child pornography from Case's computer.

4. The RoundUp computer program and its supplements can invade the private and unshared storage files of a remote computer and surreptitiously plant a tag in these files.[6]

5. The RoundUp computer program and its supplements can exploit a network protocol to invade the private and unshared storage files of a remote computer.[7]

---

[5] Special Agent Ungerer, the affiant in the search warrant affidavit, told Stephen Odenthal, a defense expert, that, during the time period identified in the affidavit, the computer was "unattended." Exhibit 2, Document 32-1.

[6] *Efficient Tagging of Remote Peers During Child Pornography Investigations*, Marc Liberatore, Brian Neil Levine, Clay Shields & Brian Lynn. Filed in *United States v. Paul Case*, Doc. 27-5. http://people.cs.umass.edu/~liberato/blog/2013/10/07/efficient-tagging-of-remote-peers-during-child-pornography-investigations/

Strengthening Forensic Investigations of Child Pornography on P2P Networks, Marc Liberatore, Brian Neil Levine & Clay Shields.
http://forensics.umass.edu/pubs/liberatore.conext.2010.pdf.

[7] *Effective Digital Forensics Research is Investigator-Centric*, Robert J. Walls, Brian Neil Levine, Marc Liberatore & Clay Shields. Doc. 27-9 at 3, cited in *United States v. Paul Case*, Reply to Government's Response to Defendant's Motion to Suppress Evidence at 9 and Defendant's Response to Government's Sur-Reply at 2, 4. The designers of RoundUp write "…but the exact extent to which can *(sic)* investigators can exploit a network protocol to gather information remotely is unsettled law."
https://www.usenix.org/legacy/events/hotsec11/tech/final_files/Walls.pdf

6. As of September 18, 2011, RoundUp was programmed to recognize 384,000 hash values of known child pornography compiled by law enforcement.[8]

7. The RoundUp program is only provided to law enforcement.[9]

8. The government refused to provide defense counsel with the RoundUp program, specifications, protocols and FBI training manuals used by the FBI and asserted that these materials were protected from disclosure by the law enforcement privilege.[10]

3.0 Offer of Proof

Case offers to prove that the "Online Covert Employee (OCE-5023)," whom the affiant claims "successfully completed downloads of five files of child pornography" from Case's computer from 2:11 AM on November 24, 2012 to 3:33 AM on November 25, 2012, was in fact an untended computer operating a

---

[8] *Measuring a year of child pornography trafficking by U.S. computers on a peer-to-peer network,* Janis Wolak, Marc Liberatore & Brian Neil Levine at 4. Filed in *United States v. Feldman*, Case 2:13-cr-00155-LA-AEG Document 27-14 at page 4.
http://www.unh.edu/ccrc/pdf/Wolak_Liberatore_Levine_2013.pdf

[9] *Forensic investigation of peer-to-peer file sharing networks*, Marc Liberatore, Robert Erdely, Thomas Kerle, Brian Neil Levine & Clay Shields at S102.
http://www.ccse.kfupm.edu.sa/~ahmadsm/coe589-121/liberatore2010-p2p.pdf

[10] On November 15, 2013, AUSA Karine Moreno-Taxman advised counsel for Case in *United States v. Feldman* that the government would not furnish defense counsel with RoundUp's program, manual, protocols and specifications on the grounds that these documents were covered by a law enforcement privilege. This claim was reasserted by AUSA Richard Frohling on January 3, 2014. Counsel for Case does not know whether the government's concealment of RoundUp and its assertion of privilege concerning RoundUp's programs, protocols and specifications is based on directives in the Department of Justice's "Federal Criminal Discovery Blue Book." *See* complaint in *NACDL v. Executive Office for United States Attorneys and United States Department of Justice*, (D.C.D.C.), Case No. 1:14-cv-00269, Document 1 (filed February 21, 2014). Case has no objection to the government responding to this Statement of Facts under seal.

RoundUp program and that this misrepresentation prevented the Magistrate Judge from evaluating the reliability of the acquisition process and the accuracy of the affidavit's basic assertions.

Undergirding this is the principle that computers are not infallible. Although numerous scientific articles by the designers of RoundUp and other computer programs used by law enforcement assure the reader of the reliability of their programs and their extensive use in investigating child pornography and security offenses, counsel has found only one published academic discussion by independent analysts which discusses the flaws in such programs. The excerpts which follow appear in this paper: Sergey Bratus, Ashlyn Lembree and Anna Shubina, *Software on the Witness Stand: What Should it Take for Us to Trust It?*.[11] And they support Case's primary argument that an evidentiary hearing must be held to establish precisely what role RoundUp played in obtaining this search warrant.

The first point that the authors make is that court give too much deference to software:

> [C]ourts tend to regard computer-generated materials as inherently trustworthy evidence, ignoring many software and platform trustworthiness problems well known to computer security researchers.
>
> Furthermore, the timing pattern of the computer program's recorded actions led us to believe that the program produced the print-outs in an automatic fashion rather than as a result of a human operating it interactively via a human-computer interface with the operator selecting appropriate actions, stopping to inspect the

[11] This paper is available at http://www.cs.dartmouth.edu/~sergey/trusting-e-evidence.pdf

> results, making determinations, forming hypotheses, and planning further actions.[12]
>
> Thus it appears that the *only* entity to "witness" the alleged violations and to produce an account of them for the court -- in the form of a series of print-outs -- was in fact an autonomous piece of software, programmed by a company acting on behalf of the plaintiffs [here, the government] and RIAA, and running on a computer controlled by this company.

Id. at 1-2. Indeed, OCE did nothing in this case. He was merely a witness to what RoundUp already supplied. Building on that reality, it follows that greater scrutiny must attend to evidence gathered through means such as RoundUp.

> Clearly, software entrusted with such an important function must be held to special, higher standards of trustworthiness. As any computer scientist (and, indeed, any programmer) knows, bugs and misconfigurations are inherent in software, including -- despite the programmers' vigorous efforts to the contrary -- in mission-critical software, and can be deadly. Defining such standards in a way consistent with the state-of-the-art knowledge of the technical, legal, and social aspects of the problem poses a multi-disciplinary research challenge. In particular, the following aspects -- at least -- must be considered:

Id. And with that mind, courts must evaluate several aspects of the software and what it is providing. This includes the trustworthiness of the software.

> How much can the software be relied on to be error-free and to operate as expected? Such questions are central to Computer Science in general, and to Computer Security in particular, and an acceptable answer should involve a consensus by computer security experts.

Without knowing how trustworthy a program is, then a fact-finder is left to his or her own biases.

> There is a certain common expectation of precision and impartiality associated with computer systems by non-specialists. However, computer practitioners themselves joke that "computers make very fast, very accurate mistakes", and exchange cautionary stories of ubiquitous computer "bugs".

It also follows that the software---here, RoundUp---then acts as a witness.

---

[12] The timing recited in the Case affidavit also suggests that the computer was untended. The search, identification and downloading is claimed to have occurred between 2:11 in the morning of November24, 2012 and 3:33 the following morning.

> Witnesses in court make their statements under oath, with severe consequences of deviating from the truth in their testimony. Witnesses are then cross-examined in order to expose any biases or conflicts of interest they might have. Computer-generated evidence comes from an entity that cannot take an oath ensuring its intent of providing the truth (only programmers directly responsible for creating that entity can do so), nor receive an adversarial examination (which would reasonably apply only to the code and function of the software).

Id. at 2-3.

From these obvious dangers, the real problem flows: we don't know what RoundUp did.

> We can only hypothesize that this comes from the perceived properties of the nature of a "machine" as something that repeatedly and reliably performs mechanical actions, or "computer" as an "idiot savant", in the public mind, as well as from daily experience with commodity electronic devices. As a society, we have been persuaded to trust machines and to rely on them, and thus to view them -- despite occasional breakdowns and errors, even dramatic ones – as inherently trustworthy, all things considered.
>
> This attitude ignores the crucial fact that computer software and systems can be and have been programmed and configured to incorporate biases and malfeasant logic that skewed their functionality and reporting output to suit the interests of their programmer or vendor. In other words, putting a bias or an expression of an ulterior motive into the form of a computer program is not unthinkable; it is not even very hard (but, as we will show, much harder to detect than to commit).
>
> A computer scientist understands that the language of a computer program does not somehow make it impossible for the speaker to "tell a lie", intentionally or unintentionally, but, on the contrary, is as open to malfeasance or honest error (such as programmers' overconfidence) as any other kind of human expression. However, the public perception appears to be that computer technology inherently adds trustworthiness to human activities, by making it harder for the humans involved to distort reality and fall to deception or self-deception.

And building on that point, is the obvious corollary: just as computer software is not infallible, neither are federal agents.[13] The fallibility of both is

[13] *See e.g.* The extensive discussion, litigation and Congressional hearings resulting from the FBI's COINTELPRO operation. The Final Report of the Select Committee criticized the conduct of the intelligence community in its domestic operations (including COINTELPRO) in no uncertain terms:

magnified when the federal agent has no idea what the program is doing or how it works or should work.

Rather, this Court must evaluate what happened here. Indeed, an evidentiary hearing is necessary to resolve the issues of what role RoundUp played in gaining this search warrant and did federal agents, using computer programs, enter the unshared space on Paul Case's computer before the search warrant? If such occurred, Case's Fourth Amendment protections were violated and issues of independent basis and inevitable discovery must be addressed.

Courts have consistently held that files in a computer's shared space are available to the public and that a defendant has no reasonable expectation of privacy in those files. Accordingly, access by agents to these shared files does not violate the Fourth Amendment. *United States v. Borowy*, 595 F.3d 1045 (9th Cir.

> The Committee finds that the domestic activities of the intelligence community at times violated specific statutory prohibitions and infringed the constitutional rights of American citizens. The legal questions involved in intelligence programs were often not considered. On other occasions, they were intentionally disregarded in the belief that because the programs served the "national security" the law did not apply. While intelligence officers on occasion failed to disclose to their superiors programs which were illegal or of questionable legality, the Committee finds that the most serious breaches of duty were those of senior officials, who were responsible for controlling intelligence activities and generally failed to assure compliance with the law.
>
> Many of the techniques used would be intolerable in a democratic society even if all of the targets had been involved in violent activity, but COINTELPRO went far beyond that...the Bureau conducted a sophisticated vigilante operation aimed squarely at preventing the exercise of First Amendment rights of speech and association, on the theory that preventing the growth of dangerous groups and the propagation of dangerous ideas would protect the national security and deter violence.

2010). In *United States v. Stults*, 575 F.3d 834, 843 (8th Cir. 2009), the Court wrote,

> We hold that Stults had no reasonable expectation of privacy in files that the FBI retrieved from his personal computer where Stults admittedly installed and used LimeWire to make his files accessible to others for file sharing. One who gives his house keys to all of his friends who request them should not be surprised should some of them open the door without knocking. As a result, "[a]lthough as a general matter an individual has an objectively reasonable expectation of privacy in his personal computer, we fail to see how this expectation can survive [Stults's] decision to install and use file-sharing software, thereby opening his computer to anyone else with the same freely available program." *Ganoe*, 538 F.3d at 1127 (internal citation omitted). *See* also *United States v. Brashear*, ¶3, Document 41-1 at 2.

However, courts have assumed that federal agents cannot enter the unshared (private) space on a suspect's computer without a search warrant. But the designers of RoundUp have written that this issue is "unsettled."[14] Before this "unsettled" issue can be briefed, the prosecution must provide convincing evidence that on no occasion, prior to the issuance of the search warrant, did federal agents enter the unshared space on Paul Case's computer. Indeed, the government's conclusory assertion that everything that happened here was lawful is no substitute for proof supporting this Court's determination of that very question.

Here is what we know: RoundUp operates on the fringes. The creators say it is "unsettled" if it can go into the unshared space. If it's unsettled some could hold to the logic that it is thus lawful. *e.g.* All that is not specifically forbidden is permitted. But the law does not operate that way when it comes to constitutional rights; instead, the principle is that which is not permitted of the government is

[14] See footnote 7, *supra*.

forbidden. So we don't know if what happened was kosher because we don't know what happened and this program and its reach is unsettled. We need a hearing.

If information from the private and unshared spaces of Case's computer either directly, indirectly or derivatively was included in the search warrant affidavit and the government either claims that it has an independent source, or that the information would have inevitably been discovered by the FBI, using only lawful investigative techniques, it must establish these defenses at an evidentiary hearing.

Dated at Milwaukee, Wisconsin, this 5th day of March, 2014.

Respectfully Submitted,

___/s/ Robin Shellow____
Robin Shellow, #1006052
The Shellow Group
324 W. Vine Street
Milwaukee, WI 53212
Tel: 414-263-4488
Fax: 414-263-4432
tsg@theshellowgroup.com

Co-Counsel: /s/James M. Shellow_____
James M. Shellow, #1006070
Shellow & Shellow, S.C.
324 West Vine Street
Milwaukee, Wisconsin 53212
Tel: 414-271-8535
Fax: 414-263-4432
jamesgilda@aol.com

Attorneys for Paul Case